PYTHON FOR EXPLOITERS COURSE

The Python for Exploiters Course challenges students to implement their own custom attack frameworks for use during penetration testing and other activities. Students will no longer need to rely on a framework written and designed by someone else during assignments, they will use a tool that they created, free of known and compromising signatures. By leveraging what they have learned in the past with Python and new concepts introduced in the course, students will design and develop a framework that is both extensible and easy to use. During this 5 day course, students will be given a sample framework which will act as a template for their own platform. Each module in the course will allow students to build upon and customize their platform while learning to convert and import new tactics and techniques. The topics covered range from simple scanners to custom browser exploitation to privilege escalation, all built into a custom framework. On the final day of the course, students will be challenged to use this newly created attack platform in a live assessment, including designing and developing new features on-the-fly to handle new challenges within the assessment range. By the end of the course, students will walk away with a framework they can use on future assessments and continue to build upon.

CHIRON METHODOLOGY DOMAIN

CYBER DEVELOPMENT PROFESSIONAL™ (CDP)™

DURATION
5 DAYS

RECOMMENDED PRE-REQUISITES

- Comfortable writing programs in Python (Python Programming Course)
- Familiarity with VMware Player or Workstation
- Experience with Red Teaming and/or Penetration Testing Techniques

PHONE: 410.672.1552 x 109 **FAX:** 410.672.3187 **ADDRESS** 7021 Columbia Gateway Dr. Suite 250 Columbia, MD 21046

PYTHON FOR EXPLOITERS COURSE

COURSE SCHEDULE

DAY 1:

LEARNING OBJECTIVES

- Understanding advantages of a custom attack framework
- Basic familiarity with structure and use of the framework
- Demonstrate the ability to create and use custom modules in the framework
- Familiarity with the use of Scapy in scanning a network

OUTLINE

- Orientation
  - Introductions
- Hacker Methodology
- Introduction to the Framework
  - Architectural aspects and maintenance implications
- Introduction to Scapy
  - Basic scripting and optimization strategies for Scapy

DAY 2:

LEARNING OBJECTIVES

- Understanding of how to create various scanners for the attack framework
- Understanding the characteristics of several well-known TCP/IP stacks
- Understanding of how to manipulate the TCP/IP stack to disguise your attacking system

OUTLINE

- Scanning
  - TCP Connect Scanner
  - TCP SYN Scanner
  - TCP ACK Scanner
  - ARP Scanner
- Passive TCP/IP Stack Fingerprinting
  - IP Headers
  - TCP Headers
- Disguising the Attacking System
  - Looking like Windows
  - Looking like Linux
  - Looking like Scapy
  - Improving your look

DAY 3:

LEARNING OBJECTIVES

- Understanding and applying enumeration and exploitation of common services on Windows and Linux using the attack framework
- Understanding and applying privilege escalation on Windows and Linux
- Familiarity with writing and using cross platform host surveys

OUTLINE

- SMB Version Scanner
- Shellshock Scanner/Exploit
- Heartbleed Scanner/Exploit
- Simple Webcrawler
- Privilege Escalation
  - Windows Techniques
  - Linux Techniques
- Platform independent host surveys in Python

PYTHON FOR EXPLOITERS COURSE

COURSE SCHEDULE

DAY 4:

LEARNING OBJECTIVES

- Understanding and implementing common approaches to persistence
- Ability to exfiltrate encrypted data from a network
- Ability to execute Python scripts in an environment without Python installed

OUTLINE

- Three levels of stealth and implementation of:
  - Windows backdoors
  - Linux backdoors
  -
- Exfiltration
  - via HTTP
  - via FTP
  - via HTTPS
  - Upload/Download
- Python binaries and executables
  - On Windows
  - On Linux

DAY 5:

LEARNING OBJECTIVES

- Apply the lessons of the previous 4 days of instruction in a private network

OUTLINE

- Scanning
- Exploitation
- Privilege Escalation
- Host Survey
- Backdoors
- Exfiltration